Department of Homeland Security Daily Open Source Infrastructure Report for 03 August 2005

Current Nationwide Threat Level is

ELEVATED
Significant Risk of Terrorist Attacks

For info click here
http://www.dhs.gov/

Please Help Improve the DHS Daily Infrastructure Report!!

We are striving to improve the DHS Daily Infrastructure Report for all of our readers. Please help us in this effort by filling out a short feedback form, which can be found by clicking on this link:

http://chrome.osis.gov/questionnaire

The form will only be available for *one more week*, so please fill it out at your earliest convenience. Your participation is important to us! Thank you.

Daily Highlights

- A report from Gartner research says that up to half of all banks don't check to see if the ATM card used to withdraw money is really the ATM card they gave the consumer, enabling phishers to take advantage of ATM card fraud. (See item 7)
- CNN reports an Air France passenger jet attempting to land at Toronto's Pearson International Airport overran a runway bursting into flames and sending smoke billowing into the sky −− all onboard survived. (See item 16)
- Reuters reports car industry officials and analysts say hackers' growing interest in writing viruses for wireless devices puts auto computer systems at risk of infection. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 02, Associated Press* — **Dynegy selling gas processing business.** Dynegy Inc. announced plans on Tuesday, August 2, to sell its natural gas processing business to Houston, TX−based Targa Resources Inc. in a cash deal of nearly $2.5 billion. The sale, approved by directors at both companies, would position Dynegy as solely a power generator primed for consolidation with other energy companies. Targa Resources, which also will acquire Dynegy's fractionation, storage, transportation, distribution and marketing assets, is a company affiliated with private−equity investor Warburg Pincus. Dynegy announced in May its intention to sell essentially half its business.
Source: http://biz.yahoo.com/ap/050802/dynegy_sale.html?.v=2

2. *August 02, New York Times* — **Chinese company ends Unocal bid.** The giant Chinese oil company Cnooc on Tuesday, August 2, ended its $18.5 billion takeover bid for the Unocal Corporation of America, citing fierce political opposition to its bid in Washington that it called “regrettable and unjustified." The decision ends a fierce takeover fight between Cnooc and the Chevron Corporation, which have both been vying to acquire Unocal’s valuable oil and natural gas assets, much of which are based in the United States and Asia. The move now clears the way for the Chevron Corporation of America to finalize its acquisition of Unocal for about $17 billion in cash and stock. Cnooc’s all−cash bid for Unocal in late June was the largest takeover bid ever attempted by a Chinese company. The month−long battle for Unocal’s assets came to symbolize the growing trade and political tensions between China. The two countries lead the world in oil consumption. However, China’s much−smaller economy is growing at a rapid clip, and so the country’s state−owned oil and energy companies have been scouring the globe in recent years for new sources of energy.
Source: http://www.nytimes.com/2005/08/02/business/worldbusiness/02cnd−china.html?hp&ex=1123041600&en=089db758ab494e9b&ei=5094&p artner=homepage

3. *August 02, Canadian Press* — **Ontario consumers urged to cut back on power use as heat, humidity returns.** Ontario, Canada's most populous province, will rely more heavily on U.S. neighbors for power this week amid soaring demand and generating stations that are down for repairs, Ontario's electricity market watchdog warned Tuesday, August 2. Five generating units were offline to undergo repair and maintenance, pulling some 3,000 megawatts out of Ontario's electricity grid, said Terry Young, spokesperson for the province's Independent Electricity System Operator. The temporary loss of that supply means Ontario was forced to rely more on imports from Michigan, New York and elsewhere to meet demand as extreme humidity once again drives up air conditioner use, Young said. "We're going to be reliant on imports today and through the week in order to meet demand in Ontario," said Young. Constraints in those U.S. states that ship surplus power to Ontario could force the province to take more drastic steps, including brownouts and rolling blackouts, Young warned. "We're seeing very high demands for electricity, you're seeing limitations in terms of our ability to supply power from Ontario generating stations, and we also have limitations on how much power we can bring in from other jurisdictions," he said.

Source: http://news.yahoo.com/news?tmpl=story&u=/cpress/20050802/ca_pr_on_na/ont_hydro_demand_1

4. *August 02, 1010wins* — **Recent heat wave sets power−use record.** Officials of electric utility Con Edison based in New York said that July set a new high for monthly electricity used by customers: 6,395,843 megawatt hours, surpassing a record set in 2002. This level of monthly power consumption for New York City and Westchester is more than the amount of electricity used in Vermont or Alaska over an entire year.
Source: http://1010wins.com/topstories/local_story_214114647.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *August 02, Vnunet* — **New phishing method hides the true Web address.** Researchers have discovered a new method used by criminals to hide the location of phishing Websites in e−mail messages. The technique uses a form that sends the users to phishing Websites after they have pushed a button. In traditional methods, phishers employ a link in the body of the e−mail message. Although regular HTML allows phishers to hide the true location of the link to a certain degree, many e−mail clients show the true address in the bottom of the window when a user holds his mouse over the message. The new method allows the criminal to hide the true location of the Website to the recipients, increasing the chance that they will believe the message is genuine and fall for the scam.
Source: http://www.vnunet.com/vnunet/news/2140637/phishing−emails−fo rmal

6. *August 02, Rutland Herald (VT)* — **Vermont investors warned of regulator scam.** Vermont security regulators are warning investors to be on the lookout for the latest global scam −− fake regulatory Websites. According to Tanya Durkee, deputy Vermont securities commissioner, the fake online sites, which appear legitimate, gather information from investors who file a complaint about an investment scam or a stock that's gone bad. She said victims have been known to be directed to the Websites through phone or mail solicitations. Durkee said it's a new twist on the "advance fee scam," where the victim is required to pay a fee or upfront costs −− or give personal account information −− before getting their money back. She said investors can avoid becoming victims by either calling the state Securities Division to determine whether the regulator, agency or securities firm is legitimate, or verify if the regulator or agency is listed on the site of the International Organization of Securities Commissions. Also, a legitimate

regulatory authority will not charge fees to help the victims of others' wrongful conduct or illegal activities and will never promote products or endorse investment deals.
Source: http://www.rutlandherald.com/apps/pbcs.dll/article?AID=/20050802/NEWS/508020376/1011

7. *August 02, MSNBC* — **Report says lax bank security allows phishers to take advantage of ATM card fraud.** A new report from the research firm Gartner Inc. says many banks are skipping an important security check, which makes it easier for criminals to forge ATM cards. Researcher Avivah Litan, author of the Gartner report, says that payment processors have told her that up to half of all banks don't check to see if the ATM card used to withdraw money is really the ATM card they gave the consumer. For years, special security codes have been embedded in the magnetic stripes on the back of every ATM card −− secrets that allow the bank to verify the authenticity of the plastic being inserted into ATM machines. But many banks don't bother checking the codes, experts say. Instead, they rely on correctly entered PINs to prove the ATM card is authentic. Withdrawals with cloned cards are known as "white card" fraud in the banking industry, because stolen data are loaded onto the back of blank, white plastic cards that look like credit cards. Often, cloned ATM cards are the end result of a successful phishing e−mail, which tricks a consumer into divulging a PIN and account number.
Information about the Gartner study:
http://www.gartner.com/press_releases/asset_133138_11.html
Source: http://www.msnbc.msn.com/id/8743446/

8. *August 02, Denver Post (CO)* — **Hackers again hit Colorado university.** A computer security breach at the University of Colorado (CU) at Boulder has left all 29,000 students, some former students and as many as 7,000 staff members vulnerable to identify theft, the school warned Monday, August 1. Hackers gained access to information on the CU−Boulder identification Buff OneCard used by students. The card contains Social Security numbers, names and photographs. The incident marks the third computer security breach at CU−Boulder since July 21. Although the potential for identity theft exists, there is no evidence that the personal information was stolen or used, and no financial information was affected, campus officials said. The breach was reported to the information technology department on Wednesday, July 27. The servers were isolated and taken off line and a forensic investigation is underway.
Source: http://www.denverpost.com/news/ci_2906977

9. *August 02, ZDNet UK* — **Cybercriminals up ante with phishing and darkmail.** The number of phishing e−mails sent to United Kingdom (UK) businesses increased by 45 percent in July, according to the latest figures from e−mail security company BlackSpider Technologies on Monday, August 1. Phishing is not the only kind of e−mail−based attack causing concern. E−mail management firm Email Systems also reports that it has registered a 400 percent rise over the last twelve months in 'darkmail.' Darkmail is speculatively targeted, unsolicited mail, and its rise threatens the efficiency of UK computer systems as well as their security. In one type of attack, a domain is targeted and then deluged with randomly addressed e−mails. Those not bounced back by the mail server are taken to be 'live' addresses which can then be attacked in other ways. Darkmail is a relatively new phenomenon, and Email Systems says it has risen in prominence recently because of "a significant increase in the frequency of e−mail attacks that target a specific domain." BlackSpider's survey, which reported that Email Systems had detected more than 360,000 emails carrying a phishing threat in July, compared to just less than

250,000 in June.
Source: http://news.zdnet.co.uk/internet/security/0,39020375,3921167 6,00.htm

10. *August 01, Tech Web News* — **Wells Fargo introduces anti−theft alerts to customers.** Wells Fargo & Co. on Monday, August 1, introduced an e−mail alert system designed to help online banking customers detect impending identity theft. The free service sends out e−mail alerts to the customer's address based on several user−set criteria, according to Wells Fargo. Some of the alerts give customers a way to track unauthorized attempts to access their bank accounts. Among the new alerts is one that notifies customers when their account has been locked after three incorrect log−in attempts. Another sends a message that lists the number of purchases over a certain amount made with the user's credit card. The e−mail alerts, said Wells Fargo, include the pertinent information, but mask key personal data. Customers may request that alerts be sent to up to three different e−mail addresses.
Source: http://www.techweb.com/wire/security/166404177

11. *August 01, Department of Treasury* — **Treasury designates three individuals linked to al Qaeda terror cell in Italy.** The U.S. Department of the Treasury on Monday, August 1, designated three individuals residing in Italy pursuant to Executive Order 13224 for providing financial and/or material support to the Moroccan Islamic Combatant Group, a group tied to al Qaeda. "Today's action targets individuals operating an al Qaeda−linked terrorist cell in Italy that recruited combatants, raised funds for terrorist activities and even planned terrorist attacks," said Stuart Levey, the Treasury's Under Secretary for Terrorism and Financial Intelligence. Ahmed El Bouhali, Faycal Boughanemi and Abdelkader Laagoub are members of a fundamentalist Islamic terrorist organization established in Cremona, Italy in 1998 with the aim of committing terrorist attacks in Italy and other countries, including Morocco and Tunisia. Information available to the U.S. Government shows the Cremona organization has contacts with al Qaeda and Ansar Al Islam cells operating in Italy and abroad. Additionally, the group has ties to the extremist organization, Moroccan Islamic Combatant Group, which was designated by the United States on November 22, 2002 under Executive Order 13224.
Source: http://www.treasury.gov/press/releases/js2668.htm

12. *July 25, Information Week* — **Visa, American Express to drop CardSystems Solutions Inc.** Visa USA Inc. and American Express Co. are cutting ties with CardSystems Solutions Inc. after a security breach at the card−payment processor exposed more than 40 million card accounts to potential fraud. It was one of the largest data−loss and −theft incidents to hit banks, information brokers, and retailers this year. Visa said last week that it was terminating CardSystems as a Visa processor, citing violation of Visa's rules for protecting cardholder data. Visa has given banks until October 31 to cease processing transactions through CardSystems. American Express is terminating its relationship with CardSystems, also effective in October. Two weeks ago, MasterCard International Inc. said it wasn't aware of any deficiencies in CardSystems' operations that could not be corrected and that CardSystems had stopped storing sensitive data in accordance with MasterCard rules. However, CardSystems must demonstrate that it's in compliance by August 31 or its status as a MasterCard processor may be in jeopardy.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=3QB0BAWXKTKBWQSNDBCSKHSCJUMEKJVN?articleID=166401772

[Return to top]

Transportation and Border Security Sector

13. *August 02, WorldNetDaily* — **Minutemen aid in arrest of 21 illegals.** The citizen group Minuteman Civil Defense Corps recently aided the Border Patrol in the capture and arrest of 21 illegal aliens attempting to cross into the United States. Founder and leader Chris Simcox called the success a "textbook weekend." "In addition to the 21 arrests we were able to rescue one person, giving them much−needed food and water until Border Patrol agents arrived to take over," he said. The group claims it has prevented more than 60,000 cases of illegal immigration −− at least 20 percent of whom had criminal records. Simcox noted it's rarely reported that hundreds, if not thousands, die every year in the desert trying to make their way onto American soil. "It is not a problem of too much security on the border that's causing folks to die; it is the lure of too little security," he said. "If our borders were secure, people wouldn't be attempting to cross hundreds of miles of desert without adequate food or water." MinutemanHQ.com −− the combined effort of the Minuteman Civil Defense Corps and the Minuteman Project −− has now established more than 25 Minuteman chapters along the U.S.−Mexico border.
Minuteman Website: http://www.MinutemanHQ.com
Source: http://worldnetdaily.com/news/article.asp?ARTICLE_ID=45569

14. *August 02, Associated Press* — **Amtrak train derails in North Carolina.** An Amtrak passenger train struck a dump truck loaded with gravel and derailed Tuesday, August 2, killing two people, police said. Both of the people who died were in the dump truck, said police spokesperson Jim Sughrue. There were no serious injuries among the roughly 200 passengers on the train, he said. The collision knocked the train's engine and two lead cars off the tracks, said Bryant Woodall, the Fire Department's assistant chief. The upended dump truck came to rest nearby. The northbound train, the Carolinian, was coming from Charlotte and headed for New York.
Source: http://www.centredaily.com/mld/centredaily/news/12284796.htm

15. *August 02, Associated Press* — **United delays filing plan to exit bankruptcy.** United Airlines said Tuesday, August 2, it has delayed filing a reorganization plan to leave bankruptcy, a move that could push its exit from Chapter 11 protection into next year. The nation's No. 2 airline said last month it expected to file a Plan of Reorganization and disclosure statement −− which together will provide a blueprint for United's exit from bankruptcy −− to U.S. Bankruptcy Court around August 1. On Tuesday, United said it will continue to work on the plan with its unsecured creditors' committee "in order to provide an additional opportunity to continue collaborating on and reviewing the complex, extensive documents as part of the overall confirmation process." The company said it expects to file the plan in about a month, delaying its previously stated goal of leaving bankruptcy sometime this fall. Carole Neville, an attorney for the unsecured creditors committee, said the committee continues to work with United on the plan. The bankruptcy court, along with United's lenders, unsecured creditors and others, must approve a reorganization plan before the carrier exits bankruptcy.
Source: http://www.usatoday.com/travel/news/2005−08−02−united−bankru ptcy_x.htm

16. *August 02, CNN* — **All survive Air France jet crash and fire.** An Air France passenger jet attempting to land at Toronto's Pearson International Airport overran a runway Tuesday, August 2, bursting into flames and sending smoke billowing into the sky. The Airbus 340,

attempting to land in a driving rainstorm, crashed into a tree−lined gully, but all passengers and crew were able to escape the flames. "There are no known fatalities" among the 297 people and 12 crewmembers who were on board, an airport spokesperson said. About 14 people suffered minor injuries, said Steve Shaw, chairman of the Greater Toronto Airports Authority. Severe thunderstorms had occurred in the area just before the crash, which occurred about 4 p.m., local time. The plane fell into a valley at the end of the runway and cracked in half, witness Corey Marx said. Vito Porto, a freelance photographer, told Global television that an explosion occurred after the crash, throwing debris for several hundred feet. Smoke billowed from the site, as scores of emergency workers sought to put out the fire with foam.
Source: http://www.cnn.com/2005/WORLD/americas/08/02/toronto.crash/i ndex.html

[Return to top]

Postal and Shipping Sector

17. *August 02, Associated Press* — **Anthrax−detecting machine to be installed at post office.** Bloomington's U.S. Postal Service mail processing center will become one of 10 in Indiana to be equipped with a high−tech device to detect anthrax powder in mail. The Biohazard Detection System is a complex piece of equipment about the size of a big photocopier. It biochemically sniffs out traces of anthrax spores that might escape from an envelope as it runs through mail−processing equipment. The equipment is to be installed in Bloomington on August 20th and operational on August 26th.
Source: http://abclocal.go.com/wls/news/080205_ap_ns_anthrax.html

[Return to top]

Agriculture Sector

18. *August 02, Capital Press (Oregon)* — **Mexico reopens border to wheat.** Mexico closed its border to California wheat in 1996 after karnal bunt, a fungal disease that reduces yields and causes an unpalatable taste in flour milled from infected wheat, was discovered in limited areas in the Desert Southwest. Although the outbreak was small and quarantined, Mexico had continued to ban California wheat for nearly a decade. In the time that California growers weren't able to ship wheat to Mexico, that country has become the second largest destination for U.S. wheat. Handlers aren't sure what immediate impacts of the border reopening could be. After nine years, Mexico is somewhat of a foreign territory for California wheat.
Source: http://www.capitalpress.info/main.asp?SectionID=67&SubSectio nID=792&ArticleID=18684&TM=7004.102

19. *August 02, Wisconsin Ag Connection* — **Quarantined deer farm tests negative for chronic wasting disease.** A white−tailed deer farm in Portage, Wisconsin, that was under quarantine since January has been cleared from having any animals with chronic wasting disease (CWD). The Wisconsin Department of Agriculture says the herd near Rosholt was recently destroyed after one of their deer was sold to a hunting preserve that had tested positive for CWD earlier. Officials say state rules require all farm−raised deer and elk to be tested for the fatal disease when they die or are killed. Specialists from U.S. Department of Agriculture's Wildlife Services

shot the 35 deer at the farm in June. The agency says the farm has been cleaned and disinfected. But since the herd was the source of a CWD−positive animal, the farm cannot be repopulated with deer or elk for five years.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=920& yr=2005

[Return to top]

Food Sector

20. *August 01, University of Massachusetts, Amherst* — **Researchers develop technique to screen for live bacteria.** University of Massachusetts, Amherst researchers have developed a molecular−based method that distinguishes live bacterial cells from dead ones. The new method adds a level of specificity to DNA detection and could be applied to a suite of pathogens, perhaps preventing massive recalls of meat carrying E. coli. The new method takes advantage of a technique called polymerase chain reaction (PCR), which scientists use to make lots of copies of a small, specific stretch of DNA. But PCR just copies the designated DNA, it doesn't indicate whether the DNA came from a cell that was dead or alive, critical information when testing food for organisms that make people sick. The researchers treated their bacteria samples with ethidium bromide monoazide (EMA). EMA will insert itself into any DNA it finds, but it can't get through the cell membranes of healthy, living bacteria. However, EMA can easily get to the DNA of a dead or dying bacterium with a damaged cell membrane. After dosing the bacteria with EMA, the researchers zapped their samples with high−intensity visible light causing the EMA to form strong, cross−linking bonds with the DNA it's tangled up in. These bonds prevent the DNA molecules from separating, so they can't be copied during PCR. Only DNA from live cells will be copied, alerting the testers to the presence of living bacteria.
Source: http://www.umass.edu/newsoffice/storyarchive/articles/19771. php

[Return to top]

Water Sector

21. *August 02, Associated Press* — **Drought triggers water limits in Oklahoma.** Officials from Rogers County, CO, Rural Water District are asking about 10,000 residents in the northwest section of the county to drastically cut back on non−essential water use because of drought conditions. The plan limits non−essential water use to two days a week. This is the district's second restriction in a week. The first lasted 48 hours while a pump was prepared. District Chairman Ed Whitaker says the restriction was necessary because the water treatment plant could not keep pace with demand. Officials say they are relying on volunteer compliance, but mandatory rationing will be imposed if the voluntary program doesn't cut water usage enough.
Source: http://www.kotv.com/main/home/stories.asp?whichpage=1&id=877 36

22. *August 02, Casper Star Tribune (WY)* — **Website records drought impact.** The National Drought Information Center, based at the University of Nebraska−Lincoln, launched a Drought Impact Monitor this week, where people from around the U.S. can log on to a Website and report the impacts of drought. The goal is to quantify and qualify impacts of drought as thoroughly as possible. This information may even be used by elected officials to classify

conditions of drought classifications that can be helpful for federal relief money to crippled areas. The Website allows people to view impacts of drought by every county in the country. People can also trace drought history, by entering in a certain time period they are interested in seeing. In addition, people around the country will be able to input their own drought impacts, such as monetary loss.
Drought Impact Monitor: http://droughtreporter.unl.edu/
Source: http://www.casperstartribune.net/articles/2005/08/02/news/wyoming/9aa1575cbda3d9928725704f002105c7.txt

[Return to top]

Public Health Sector

23. *August 02, Bloomberg* — **China pig−borne disease deaths rise.** The death toll caused by a pig−borne disease in southwest China's Sichuan province rose to 36 as of noon Monday, August 1, China's Ministry of Health said. The number of reported infections rose by 17 to 198. The illness is believed to be streptococcus suis, a bacteria carried by pigs, the government said. The outbreak in the past two weeks has affected mostly pig farmers and butchers in the country. China is the world's largest pork producer, with most pig farming done in Sichuan and the northern province of Henan. "We feel that you can't discount immediately the presence of other bacteria, perhaps a virus, some sort of toxic event in the environment which is also making these people ill," Bob Dietz, a spokesperson of the World Health Organization, said in a Bloomberg interview. "If in the end, it turns out that it was just streptococcus suis type II, we still won't have a good understanding of why this stuff grew to such large proportions, this is unprecedented to what we have seen," Dietz said.
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=alLJ4VE31ypg&refer=asia

24. *August 01, Reuters* — **Russia bird flu could spread to European Union.** A strain of bird flu dangerous to humans could spread to parts of the European Union from Siberia, a senior Russian veterinary official warned on Monday, August 1. Chances were "very high" the strain found in the Novosibirsk region could spread to other parts of Siberia, the official from the Russian Veterinary and Phytosanitary Inspection Service told Reuters. "There is also a possibility that bird flu could spread to the European Union as (infected) wild birds from China may have been in contact in Russia with birds that will fly on to the Netherlands, France, and elsewhere," the official said. The official said it had been confirmed on Friday, July 29, that birds in the Novosibirsk region were infected with the H5N1 strain of bird flu, which is dangerous to humans.
Source: http://cnn.netscape.cnn.com/ns/news/story.jsp?id=20050801105800002326924&dt=20050801105800&w=RTR&coview=

25. *July 28, University of Chicago Hospitals* — **Studies reveal how plague disables immune system.** Two studies by researchers at the University of Chicago show how the bacteria that cause the plague manage to outsmart the immune system and how, by slightly altering one of the microbe's tools, the researchers produced what may be the first safe and effective vaccine. Both studies focus on aspects of the type−III pathway, a molecular syringe that Yersinia pestis, the plague bacteria, uses to disable its host's immune system. Bubonic plague is spread by the

bites of infected fleas, which acquire the germ from infected rodents. In the mid−14th century, the plague swept through Europe killing nearly one−third of the population. It returned with a slightly reduced death count about once a generation for centuries. Although far less common now, the plague has not entirely gone away. There are fewer than 2,000 cases a year worldwide, including 10 to 20 each year in the western U.S. One out of seven persons infected dies. Many people have worried that terrorists could exploit Y. pestis as a weapon, spreading it as an aerosol. Contracted this way −− infecting the lungs rather than the bloodstream −− the disease is known as pneumonic plague. This form of the infection progresses faster, spreads easier from person to person, and is far more deadly, killing 100 percent of those who do not receive the right antibiotics soon after exposure.
Source: http://www.uchospitals.edu/news/2005/20050728−plague.html

[Return to top]

Government Sector

26. *August 01, Department of Homeland Security* — **Operation Community Shield yields 582 arrests.** On Monday, August 1, Department of Homeland Security Secretary Michael Chertoff and Marcy Forman, Director of Investigations for U.S. Immigration and Customs Enforcement (ICE), announced the arrest of 582 street gang members and associates during a two−week, nationwide enforcement action under the auspices of “Operation Community Shield,” ICE’s ongoing national anti−gang initiative. Gang violence and gang criminal behavior is the kind of threat to our vulnerabilities that all of us −− federal, state and local officials −− are very, very concerned about," said Chertoff. "Indeed, our threat assessments indicate that many gang members come to this country from overseas, or from other parts of the North and South American continent, which means that they are subject to our immigration laws and that when they violate those laws, we can take action against them. We are deeply committed to enforcing these immigration laws and restoring integrity to our immigration system."
Remarks by Secretary Chertoff: http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0712.xml
Source: http://www.dhs.gov/dhspublic/

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information Technology and Telecommunications Sector

27. *August 03, ZDNet* — **DHS calls for tech industry involvement.** Support Anti−Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 provides government−authorized companies with immunity from civil lawsuits if their anti−terrorism products fail to perform. In order to get on the approved list, companies must first go through a two−step application process. But only 17 offerings −− none related to information technology −− have received

such approval. In a speech at the Commonwealth Club in Santa Clara, CA, Thursday, July 29, Department of Homeland Security (DHS) Secretary Michael Chertoff said the newly created position of assistant secretary for Cyber and Telecommunications Security would be in charge of stepping up the government's collaboration with tech companies. So far, none of the approved services pertain specifically to information technology security. The latest technology to make the list was a cargo container inspection system for use at ports. DHS is eyeing technological advances to beef up border enforcement, emergency preparedness, transportation and cybersecurity, Chertoff said. "But there is a way forward," Chertoff said, pointing to high−tech biometric identifiers and radio frequency identification tags as potential new avenues for screening.
A transcript of Secretary Chertoff's remarks is available on the DHS Website:
http://www.dhs.gov/dhspublic/display?content=4700
More about the SAFETY Act of 2002:
https://www.safetyact.gov/DHS/SActHome.nsf/Main?OpenFrameset &6EWVEC
Source: http://news.zdnet.com/2100−1009_22−5814289.html

28. *August 02, FrSIRT* — **jabberd "jid.c" JID handling remote buffer overflow vulnerabilities.** Three vulnerabilities were identified in jabberd, which could be exploited by remote attackers to execute arbitrary code or cause a denial of service. These flaws are due to buffer overflow errors in "jid.c" when processing JID strings with long components (user, host or resource), which may be exploited to compromise a vulnerable system or cause a DoS. jabberd versions prior to 2.0s9 are affected.
Users should upgrade to jabberd version 2.0s9: http://jabberd.jabberstudio.org/2/
Source: http://www.frsirt.com/english/advisories/2005/1286

29. *August 01, Reuters* — **Car computer systems at risk to viruses.** Car industry officials and analysts say hackers' growing interest in writing viruses for wireless devices puts auto computer systems at risk of infection. As carmakers adjust on−board computers to allow consumers to transfer information with MP3 players and mobile phones, they also make their vehicles vulnerable to mobile viruses that jump between devices via the Bluetooth technology that connects them. The worst that could happen is that the computer's control of engine performance and emissions, navigation and entertainment systems cease to function. That would probably mean an annoying trip to the repair shop or having to reboot the system. Companies so far have seen no reports of viruses in auto systems, and studies have shown it is not easy to transplant a virus into a car, but carmakers say they are taking the risk seriously. The first mobile phone virus, Cabir, has spread to over 20 countries, ranging from the United States to Japan and from Finland to South Africa, using only Bluetooth. Bluetooth is used in car electronics interfaces for monitoring and service. Carmakers say they use the most sophisticated protection for safety equipment such as airbags or motor controls, whereas infotainment systems so far have less stringent safeguards.
Source: http://www.cnn.com/2005/TECH/08/01/viruses.cars.reut/index.h tml

30. *August 01, Techworld* — **Hackers break into Microsoft's anti−piracy system.** Hackers found a way around Microsoft's Windows Genuine Advantage (WGA) anti−piracy system last week, only a day after the system went into effect. WGA requires Windows users to verify they are using a genuine copy of Windows before they are allowed to download certain software updates. Security patches aren't covered by the system, and remain available to any Windows

user, legitimate or not. Using a simple JavaScript hack, all users had to do was paste a JavaScript URL into the Internet Explorer browser window at the beginning of the process; this turned off the key check, according to users. Microsoft said it was investigating the hack but didn't consider it a security flaw. The company said that it may not take immediate action to fix the problem. "As the validation system is updated from time to time, we will address this and other issues that may arise," a Microsoft spokesperson said. Microsoft put WGA into place to cut down on Windows piracy, and to persuade users who are running pirated copies of Windows to buy legitimate licences.
Source: http://www.techworld.com/security/news/index.cfm?NewsID=4134

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: A presentation at Defcon entitled "Live penetration Test of the Backbone" was scheduled to include use of an exploit disclosed by Michael Lynn earlier this week. The exploit is NOT the weak version demo'd by Lynn, but a fully working version that is capable of re−routing traffic, man in the middle and / or dropping the router. EFF lawyers toned down the presentation to avoid ISS and/or Cisco lawsuits. Analysis: There is an exploit. It will fall into the wrong hands. Prepare your Networks. RECOMMENDATIONS AND COUNTERMEASURES If your network doesn’t need IPv6, disable it. This will eliminate exposure to this vulnerability. On a router which supports IPv6, disable it by issuing the command "no ipv6 enable" and "no ipv6 address" on each interface. On those systems that do require IPv6 capabilities check the Cisco advisory information to determine vulnerability and countermeasures.
http://www.cisco.com/warp/public/707/cisco−sa−20050729−ipv6. shtml

Current Port Attacks

Top 10 Target Ports	1026 (−−−), 445 (microsoft−ds), 27015 (halflife), 139 (netbios−ssn), 6881 (bittorrent), 25 (smtp), 135 (epmap), 80 (www), 3800 (−−−), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer